DRAFT MINUTES
Commonwealth of Virginia
Identity Management Standards Advisory Council (IMSAC)
General Meeting for Public Comment
Monday, July 16, 2018

Commonwealth Enterprise Solutions Center
Multipurpose Room 1222
11751 Meadowville Lane
Chester, VA 23836

ATTENDANCE

Members Present:

Lisa Kimball, Chairperson
Katie Crepps

Michael Watson

Jeremy Grant – via conference call from Washington, DC
Lana Shelley – via conference call from Richmond, VA

Staff Present:

Karen Baldwin, VITA / IMSAC staff
Joseph W. Grubbs, PhD, VDOT
Chelsea Jackson, VDOT
Greg Richards, OAG

Members Absent:

Nelson Moe
Tom Moran
Jeffery Zubricki

Note: The IMSAC Meeting Materials may be accessed on the VITA website at:

https://www.vita.virginia.gov/about/councils-committees/imsac/meeting-materials/

Call to Order

Chairperson Kimball called the meeting to order at 11:17a in multipurpose room 1222 at the Commonwealth Enterprise Solutions Center in Chester, VA.

Roll Call was taken for IMSAC members. All members were present except Mr. Zubricki, Mr. Moran and Mr. Moe; however, a quorum was not reached. Chairperson Kimball noted that the Council would not entertain any motions nor would they take anything under advisement for approval.

Meeting Minutes

Approval of meeting minutes from the May 24, 2018 meeting will be added to the agenda for the next scheduled meeting where a quorum is present.

Discussion of Proposed Approaches for Certification of Trust Framework Operators pursuant to the Electronic Identity Management Act, IMSAC Guidance Document 5: Certification of Trust Framework Operators

Dr. Joseph Grubbs, IMSAC Subject Matter Advisor
Virginia Department of Transportation

Dr. Joe Grubbs conducted a review of the provisions and content of Guidance Document 5.

Staff reviewed and edited the document, correcting and updating the document primarily for wordsmithing objectives.

Dr. Grubbs described the business need for Trust Framework Operators to demonstrate compliance with adopted minimum specifications and standards under the Electronic Identity Management Act, affording them with qualification for liability protection. Without a certification process: determination of compliance will remain subjective and open to dispute; the courts will be unnecessarily burdened with determination of compliance for each petition for liability claim.

Guidance Document 5 (GD 5) establishes objective, consistent criteria for evaluating TFO compliance based on adopted minimum specifications and standards. The Document also enables setting of requirements for TFOs to maintain an audit of compliance as part of the certification process, and provides the courts with objective criteria based on adopted minimum specifications and standards to evaluate liability claims and determine whether TFO has been compliant. GD 5 also remains consistent with statutory provisions and limitations in the Act, and is consistent with the intent of the IMSAC. The guidance document aligns with the European Union's standards-based model for certification established in the eIDAS and applies criteria for certification authorities consistent with the EU's eIDAS Regulation #910/2014.

Dr. Grubbs offered three discussion points to the group for consideration prior to recommending GD 5 for adoption:

- Liability of certification authorities pursuant to the Act;
- Contracts between TFOs and candidate certification authorities;
- Limitations in the Act to address (or accommodate) federation.

Katie Crepps added that the minimum guidance for the certification process can include a 'point in time' aspect, where the Council could recommend that certification be renewed within or not to exceed a specific time period. Providing minimal guidance on the timeline may be the right path for the Council. Adding a statement around certification might be difficult because assessing where a 'bad actor' may occur is challenging without considering many scenarios around where the 'bad actor' could occur. TFOs and certification authorities are required to notify the Council and Commonwealth Security when a breach occurs; Ms. Crepps inquired whether this info is available publicly in EU: Dr. Grubbs answered 'yes'. Chairperson Kimball asked whether GD 5 should be reviewed for compliance with the General Data Protection Regulation (GDPR)? Dr. Grubbs: we have discussed this with General Counsel and staff has worked to keep guidance documentation consistent with current regulations. Mr. Grant stated that continuing to model guidance language around eIDAS is the right path.

The second discussion point describes warranties between TFOs and candidate certification authorities. Dr. Grubbs stated that the guidance language is not something that should be added; language around liability would become too prescriptive and would exceed limitations in statute; recommendation is that it should be left out.

The third point: lingering issue that the Act does not accommodate federation, which is limiting. Large issue around federation that has not been addressed. Federation would allow users to certify once and use ID many times. SB 1269 attempted to address this but was not passed. Ms. Crepps: how limiting? Credentials have to be validated; to access validation through trust framework, some agreement has to exist between TFOs to do validation. Once this exists, does it become consolidated trust framework? Would we consider them one entity? Dr. Grubbs: depends on what is nature of agreement? Existing guidance is for initial enrollment and issuance of certification. Recognized as singular network? Dr. Grubbs deferred to Greg Richards with OAG for legal points. Mr. Richards: draft guidance document on federation; once Act is modified to recognize federation, guidance document can reflect requirements for recognizing certification of TFOs between certification authorities. Dr. Grubbs: guidance document is ready but cannot move forward without modification of the Act. Following staff rework, anticipate bringing modified document back to Advisory Council for action.

Chairperson Kimball: if there are no objections, breaking for lunch, to return at 1p.

Note: draft watermark should be removed from Agenda, as this is the final Agenda.

Chairperson Kimball reconvened the meeting at 1p.

Reminder: we do not have quorum, so we will not take anything under advisement or make any decisions.

Chairperson Kimball requested that Mr. Richards ensure that public comments are handled appropriately, and to guide the discussion for the afternoon session.

Chairperson Kimball provided a Recap: The Electronic Identity Management Act that was passed in 2015 was silent on federation and intentionally specific to the Commonwealth of Virginia. In 2017, this body took the initiative to draft an amendment to the Act to add language to include the concept of federation. Public comments were received on the draft amendment to explicitly add protections for framework operators and certification authorities. These "eleventh-hour" changes did not allow sufficient time for analysis and education of interested parties; the proposed amendments to the legislation "died in committee". The Council, which has the goal of updating the Act in the 2019 legislative session, intends to re-propose the original draft language to add federation to the 2015 Act without otherwise changing the substance or intent of the Act. It was noted that IMSAC documents (specifically Guidance Doc 5) require some rework to ensure that all guidance is in synch with the proposed legislative changes.

Mr. Richards: the process last session was rushed and not effective; the Council will work to ensure that talking points are concise and are effectively communicated to interested parties.

Chairperson Kimball requested input from Council; is adding 'federation' appropriate at this point?

Mr. Grant: no objection; thought that original intent was to include federation, and this should be pursued.

Chairperson Kimball: Mr. Shorter, please feel free to comment.

Mr. Scott Shorter (representing the Kantara Initiative): Which documents are we discussing? Proposed redlines or other? When reviewing the redlined document, what is disposition of public comments proposed? We saw changes in paragraphs regarding federation or federated digital identity system. Is italicized text new proposals to legislation from Council?

Mr. Richards: separate proposal that Council agreed upon, introduced by VITA Legal and Legislative Affairs directly to Delegate Levine; following that, Kantara introduced to Delegate Levine a proposed substitute. Italicized text is effort to return legislation to original legislation that Advisory Council adopted. Italicized language is new and came from Kantara.

Mr. Shorter: we originally proposed five bullets, now there are three; can we discuss rationale for deletion of two bullets?

Mr. Richards: a number of Romanettes that were subsumed were duplicative of other wording in legislation in terms of creation and limitation of liability, intention was to not have an overly-complicated list of definitions.

Chairperson Kimball: italicized text was what was originally proposed, eliminating Romanettes was to eliminate duplication and remove confusion. Regarding the paragraph that was stricken in document: that language was premature and detracted from the goal of adding federation to the Act because it introduced private interest protection into the legislation.

Mr. Shorter: would Federation apply to Certification Authorities and Trust Framework Operator definitions?

Chairperson Kimball: yes.

Mr. Shorter: should we understand that these roles definitions were subsumed into TFO? Or which existing entity performs the federation?

Chair Kimball: here is where I become concerned with trying to legislate standards and frameworks, believe that as the documentation matures, as standards become more comprehensive body, all those will be fleshed out and understood, and I am concerned about including that language or prepare or that language within the Act.

Mr. Richards: there are statutory definitions for TFO in the legislation for those roles, and for various other roles: identity proofer, provider, etc. While I haven't looked at the definitions in a while, whether what is proposed for administrator or operator, whether what is proposed actually fits, I cannot speak to that.

Mr. Shorter: get federation in the door, complexify it later. Next steps?

Chair Kimball: adding federation to the legislation enables us to do a lot of the work we want to do, from a standards and definitions standpoint, so we can move forward with a lot of those thoughts. If additional legislative changes are required or there are ancillary proposals, I believe that can happen because we will be building both sides of the equation concurrently.

Mr. Grant: can I ask a question? Perplexing that we did not have federation in this initial legislation, since it seemed clear from the original Act a few years ago that this was covered given the definitions included. Understanding that we have a different interpretation right now, do we have validation from the AG's office that this will solve the current concerns? I don't want to be in a situation a few years from now to have to redefine things more specifically to ensure that the original intent of the statute will be honored.

Mr. Richards: (go to Section 59.1-550 through 555): when working through this, we recognized that the Electronic Identity Management Act certainly discusses relying parties, and it may have been contemplated that the legislative proposal accomplished federation, but when you get into establishment of liability and limitation of liability provisions it only applies to the issuance of an identity credential.

Mr. Grant: if we have this language in the legislation, will it address the concerns?

Mr. Richards: yes, absolutely.

Chair Kimball: Scott, we have the definitions on the screen here if you wish to review.

Mr. Shorter: understand now why the edits to the edits were made; what Kantara is trying to get at and why they added these roles is what as an entity is their position with respect to the legislation? Seems like Kantara initiative, with identity assurance framework, is a TFO, but also seems like they are certification authority which does audit of something called identity trust framework operator. Is there another layer envisioned where a certification authority will come in and audit Kantara's operations to ensure that they are approving credential service providers through proper procedures or not? Where liability lands is an important question for them.

Chair Kimball: The Council wants to keep the Framework and supporting documents as simple as possible. We do not intend to task any organization within the Commonwealth with policing adherence. The CIO and CISO had indicated that the Commonwealth does not want to have that role.

Mike, correct me if I'm wrong – is that not what you and Nelson said - that the Commonwealth does not want to end up with the responsibility of certifying the certifiers etc.?

(conference call dropped)

Mr. Shorter: is there any entity in that role or is that how you saw the Kantara's of the world?

Mr. Watson: referencing certification process in document 5?

Mr. Shorter: correct

Mr. Watson: I think the intent as part of certification process, don't believe there is a specific reference except that what goes through the certification process; if someone finds that the TFO is not compliant with processes, presumption is that they open themselves to liability?

Mr. Richards: what I think I hear is that there is an assumption is that the liability that could be imposed on TFO could be shifted to certification authority; but this is difficult to assess since the guidance document is incomplete and legislative approach for 2019 session is not available.

Mr. Watson: not looking for auditor; if organization meets requirements, then they are protected from liability; if they don't meet requirements, they would then assume liability.

Mr. Shorter: so Kantara would be protected from liability assuming they continue to meet requirements for certification?

Mr. Watson: yes

Ms. Crepps: auditability is the goal, not having to have an auditor come in. When the bad actor events occur, a post mortem usually occurs to see who was the bad actor. We are leaning toward a 'minimum guidelines' approach; establish minimum requirements to be met and self-assess toward them while maintaining auditability. If that can't be proved, the organization is liable.

Mr. Shorter: it should not be inferred that there is a type of entity called a certification authority which is assuming all the liability risk that other entities are evading?

Ms. Crepps: I don't think that is a good assumption.

Mr. Shorter: can language be included to clarify that there is an entity called certification authority with these responsibilities, move responsibilities from TFO to certification authority?

Chair Kimball: the Council is concerned about attempting to include all the possibilities within the legislation itself; we endeavor to ensure that the associated applicable standards are as clear as possible.

Mr. Shorter: if certification authority is a different entity, propose that it be listed as a separate entity.

Chair Kimball: understand that. Greg, thoughts on this?

Ms. Crepps: are you proposing that a certification authority could not be a TFO? Because they could – an organization can choose to operate the two independently. They don't have to be mutually exclusive, as two separate entities - they could serve as both.

Mr. Shorter: they have distinct swim lanes, thought they were separate entities. Could Guidance Document 5 clarify?

Ms. Crepps: definitions for TFOs and Cert Authorities are not the same

Chair Kimball: to clarify, the actions and/or the activities are separate, as opposed to having to be individual entities. Does that help?

Mr. Shorter: yes – so Kantara can continue to think of itself as a TFO that performs certification authority activities; that doesn't make it stop being a TFO if it complies with this language. If fully-compliant in both roles, Kantara would maintain the protection afforded by the Act.

Chair Kimball: yes, that has always been the intent. Kantara (and other organizations, of course) could serve in both roles and maintain the limited liability protection in the Act.

Ms. Crepps: there is nothing in here that precludes that.

Mr. Shorter: and other types of entities could also become a CA

Mr. Shorter: we would love to see certification authority more clearly defined.

Chair Kimball: comments on definitions are welcome, along with comments, suggestions and all input on each of the Council's work products. Our intent is to use common terminology across all documents related to the legislation.

(conference call restored)

Mr. Shorter, et al: <recapped conversation since call dropped.>

Ms. Crepps: I think where we settled was that TFO and CA are two separate roles not necessarily entities; not mutually exclusive; feedback around definition of certification authority indicates that we need to clarify this.

Chair Kimball: thank you to Kantara for feedback and input. As we look at GD 5, anyone with ideas on how to better illustrate the roles and entities, please provide comments. Our recommendation to Mr. Link, is to revert to the amended legislation proposal from last year that was drafted simply to add Federation language, and then see if Kantara – and all other interested partied, of course - has additional changes or inclusions – is that doable?

Mr. Richards: I can put together a redlined version for discussion by the Advisory Council and for approval to send forward.

Chair Kimball: I believe he needs a draft by August?

Mr. Richards: yes

Chair Kimball: we will explore options, as the Council will not be meeting until September or October. Also want to provide opportunity for public comment. Also asking for suggestions on the talking points, to have available for input.

Ms. Crepps: a diagram would be useful if added to Talking Points.

Mr. Richards indicated that he has a diagram that could be added.

Chair Kimball: any other comments? Anything else to share?

Mr. Grant: helped launch the Better Identity Coalition, developing policy blueprint. Hosting event on Thursday; betteridentity.org.

Adjournment

Chairperson Kimball asked the Advisory Council if there were any objections to adjourning; hearing none, the Chair adjourned the meeting at 1:48 p.